International National Standard Application (INTL NSA) – Privacy Impact Assessment

PIA Approval Date – December 11, 2009

System Overview:
International National Standard Application (INTL NSA) is an application that captures tax information related to foreign individuals and entities (e.g. foreign partnerships, corporations, etc.). The tax withholdings are reported on various tax international returns prepared by or for those foreigners or foreign entities, and then submitted to the IRS. There are four modules/subsystems which facilitate the capturing of this data, and they are Project 1446 NSA 36, Foreign Investment Real Property Tax Act (FIRPTA) NSA 37, Elections NSA 40, and Form 8233.

Systems of Records Notice (SORN):
- IRS 34.037--IRS Audit Trail and Security Records System
- IRS 42.001--Exam Administrative Files
- IRS 42.021--Compliance Returns and Project Files

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer – For purposes of this PIA, the "taxpayer" can be either an individual or a business entity.

- Full Name
- Address
- Taxpayer Identification Number (TIN)
- Entity Information of a Foreign Corporation

- Data from Forms 8288 and 8288–A:
  - International Tax Returns
  - Tax Withholdings

- Additional Data from Form 8804:
  - Withholding Agent Name
  - Withholding Agent Address
  - Taxpayer Liability and Payments

- Additional Data from Form 8805:
  - Foreign Partner's Full Name
  - Foreign Partner's U.S. Identifying Number
  - Partnership Name
  - Partnership Account Number
  - Withholding Agent's U.S. Identifying Number
  - Effectively Connected Taxable Income (ECTI)
  - Beneficiary Full Name
  - Beneficiary Address
  - Beneficiary U.S. Identifying Number
  - Tax Credit

- Additional Data from Form 8813:
  - Employee Identification Number (EIN)

- Additional Data from Form 8233:
  - Foreign Tax Identifying Number
  - Tax Exemptions
  - Immigration Status
  - Passport Number

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS – The forms listed in Question 1 that are on file with the IRS are used to populate data in the system.

B. Taxpayer – The forms listed in Question 1 are sent to the IRS by taxpayers and are used to populate data in the system.

3. Is each data item required for the business purpose of the system? Explain.
Yes. The International NSA (FIRPTA, Elections, Project 1446, 8233) database is designed to collect relevant data to the processing of Forms 8288-A, 8805, 8288-B, 8233 and 897(i) Elections. This data is used in corresponding with taxpayers, researching for up-front credit verification, and transmitting data records to the Compliance Data Warehouse (CDW), the office of Statistics of Income (SOI), and the Enterprise Computing Center in Martinsburg (ECC-MTB) for upload to the Information Returns Master File (IRMF). Employee data is maintained strictly for the purpose of identification and authentication.

4. How will each data item be verified for accuracy, timeliness, and completeness?
All of the data enters this module/subsystem via manual data entry. The system maintains accuracy, completeness, and validity of information by packets, checksums, and encryption. The application performs validations as defined by the business owner as applicable. Validation tables are built into the system where applicable. Validation tests are performed between related data elements for accuracy. The application performs validity and consistency checks. Informational messages are provided for the accurate and complete input of the data. Checks are built into the application to ensure that the data is fully qualified and that the data type is accurate. No data will be saved to the database that has not fully passed the validation checks.

5. Is there another source for the data? Explain how that source is or is not used.
No, the tax forms listed in Question 1 are the sources of the data in INTL NSA.

6. Generally, how will data be retrieved by the user?
The user can retrieve the data by document locator number, file control number, taxpayer identification number, date of transfer, amount realized, property description, taxpayer name, partnership employer identification number (EIN), foreign corporation EIN, or election control number.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes, the data is retrievable by taxpayer name and identification number.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
There are no external interfaces and only IRS personnel have access to this application via the IRS Intranet. Authentication is provided by Active Directory and INTL NSA authentication. A list of users and their job descriptions is below:

- End–User 1:
  - Project 1446
  - FIRPTA
  - Elections

    Role: Wage and Investment (W&I) FIRPTA Unit Clerks
    Permission: Conduct manual data entry and issue FIRPTA cover letters

    Role: Tax Examiners (TE)
    Permission: Prepare the source documents to be entered into the application and review existing documentation.

- End–User 2:
  - Form 8233

    Role: W&I Unit Clerks
    Permission: Read, write and research capabilities.

    Role: Tax Examiners (TEs)
    Permission: Read, write and research capabilities

    Role: Customer Service Representatives (CSR)
    Permission: Read, write and research capabilities

    Role: Leads and Managers
    Permission: Review employee work

- End–User 3:
  - Project 1446
  - FIRPTA
  - Elections
  - Form 8233

    Role: W&I Headquarters (HQ) Analysts
    Permission: Read, write and research capabilities

    Role: Large and Mid–Size Business (LMSB) Revenue Agents
    Permission: Research capabilities

    Role: Small Business/Self–Employed (SB/SE) Revenue Agents
    Permission: Research capabilities

Role: Revenue Officer Unit Clerks
Permission: Research capabilities

Role: TEs
Permission: Read, write and research capabilities

Role: CSRs
Permission: Read, write and research capabilities

Role: Unit Leads
Permission: Read, write and research capabilities

Role: Managers
Permission: Read, write and research capabilities

- Administrators:

  Role: System Administrators (SAs)
  Permission: Read, write for the purpose of troubleshooting

  Role: Database Administrators (DBAs)
  Permission: Read, write for the purpose of troubleshooting

- Developers:

  Role: Developers
  Permission: Situational access to read, write and delete (only in development)

9. How is access to the data by a user determined and by whom?
INTL NSA relies on user identification and authentication (I&A) controls implemented for the IRS Intranet on MITS–17 via Active Directory (AD). Users are identified and authenticated for access to the network via Standard Employee Identification (SEID) and password. A list of local user accounts is maintained within the operating system and in the Online 5081 system. Aelita software identifies accounts that never expire, and sends alerts to the security analyst for confirmation with the manager for that user. End User Equipment and Services (EUES) group performs account management activities, e.g. adding and deleting user accounts for logon domains. (Refer to Modernization and Information Technology Services [MITS]–17 SSP for detailed user account management controls at the domain level.)

First, users logon to the IRS local area network (LAN) and authenticate with their LAN authentication credentials. Once authenticated, the user then logs onto a UNIX server where upon successful authentication, there will be an icon for INTL NSA. If the user wishes to logon to INTL NSA, they must click the icon and enter a separate authentication credential.

Only users with a business need to know are granted access to INTL NSA. Users must prepare an On Line 5081 (OL5081) request, which is approved by the user's manager, in order to gain access to the system.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
No, other IRS systems do not provide, receive, nor share data with INTL NSA.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Not applicable.

12. Will other agencies provide, receive, or share data in any form with this system?
No, INTL NSA does not provide, receive, nor share data with other agencies.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
The application relies on the MITS–24 General Support System (GSS) for the implementation of this control. Refer to the MITS–24 GSS SSP for additional information. Temporary tax form data is required to be retained for six years, according to Internal Revenue Manual (IRM) 1.15.2.3. Audit trail archival logs for data are retained as specified by a system records retention schedule in accordance with IRM 1.15, unless otherwise specified by a formal Records Retention Schedule developed in accordance with IRM 1.15, Records Management. Audit logs may be retained up to seven (7) years.

- **FIRPTA:** Forms 8288/8288–A – Destroy paper and electronic files 7 years after the end of the processing year. Form 8288–B – Destroy paper and electronic files 6 years after the case is closed. See IRM 1.15.29, Exhibit 1.15.29–1, Items 75 and 223.

- **Project 1446:** All taxpayer electronic file data is destroyed when it has reached the 6th year after the end of the processing year as required by IRM 1.15.29. The records are extrapolated and then erased/deleted from the UNIX box. The data cannot be recovered. Refer to IRM 1.15.29, Exhibit 1.15.29–1, Item 56, Job No. N1–58–95–1.

- **Elections:** Records Control Schedule for Tax Administration – International, Exhibit 1.15.26.1, Item 23: Retire to the Federal Records Center 2 years after case is closed; Destroy 12 years after case is closed.

- **Form 8233**: Records Control Schedule for Tax Administration – International, Exhibit 1.15.26.1, Item 6: Retire to the Federal Records Center 1 year after case is closed; Destroy 6 years after case is closed.

14. Will this system use technology in a new way?
No. The system will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No. The system will not be used to identify or locate individuals or groups.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
No. The system does not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. This system cannot be used to treat taxpayers or employees differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Not applicable.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
No, the system is not web–based.

View other PIAs on IRS.gov